THAT WHICH IS CLAIMED IS:

1. An authorization device, comprising:

an integrated circuit component that in response to a first data stream generates a second encrypted data stream which is at least periodically evaluated during a first time interval to assess whether operation of a programmable logic device during the first time interval is authorized.

2. The authorization device of Claim 1, wherein the first data stream and the second encrypted data stream are time division multiplexed on an I/O pin associated with said integrated circuit component.

3. The authorization device of Claim 1, wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream.

4. The authorization device of Claim 3, wherein said integrated circuit component comprises circuitry that intentionally inserts errors into the second encrypted data stream.

5. The authorization device of Claim 3, wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream.

6. The authorization device of Claim 5, wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit.

7. The authorization device of Claim 6, wherein the encryption operation generates a second permuted bit as a function of a second bit in the first data stream and at least the second encrypted bit in the second encrypted data stream.

8. The authorization device of Claim 7, wherein the encryption operation uses the encryption key to generate a third encrypted bit in the second encrypted data stream from the second permuted bit and the first permuted bit.

9. The authorization device of Claim 4, wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream.

10. The authorization device of Claim 9, wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit.

11. The authorization device of Claim 2, wherein said integrated circuit component utilizes an encryption operation to generate the second encrypted data stream from the first data stream.

12. The authorization device of Claim 11, wherein the encryption operation generates a first permuted bit as a function of a first bit in the first data stream and at least a first encrypted bit in the second encrypted data stream.

13. The authorization device of Claim 12, wherein the encryption operation uses an encryption key to generate a second encrypted bit in the second encrypted data stream from at least the first permuted bit.

14. The authorization device of Claim 1, wherein the first data stream is an at least weakly random sequence of bits.

15. The authorization device of Claim 4, wherein the first data stream is an at least weakly random sequence of bits.

16. An integrated system, comprising:

an authorization device that generates a first encrypted data stream;

a programmable logic device that generates a second encrypted data stream while simultaneously operating under at least partial control of configuration data during a first time interval; and

authorization detection circuitry that at least periodically compares the first and second encrypted data streams during the first time interval and disables operation of said programmable logic device if the first and second encrypted data streams indicate that said programmable logic device is not authorized to utilize the configuration data.

17. The system of Claim 16, wherein said programmable logic device generates an at least weakly random data stream during the first time interval; and wherein said authorization device generates the first encrypted data stream in response to the at least weakly random data stream.

18. The system of Claim 16, wherein said authorization detection circuitry is internal to said programmable logic device; wherein said programmable logic device utilizes an encryption operation to generate the second encrypted data stream; and wherein each of a plurality of bits in the second encrypted data stream is determined by evaluating at least one bit in the first encrypted data stream.

19. The system of Claim 17, wherein said authorization detection circuitry operates as a dead man switch internal to said programmable logic device; wherein said programmable logic device utilizes an encryption operation to generate the second encrypted data stream; and wherein each of a plurality of bits in the second encrypted data stream is determined by performing the encryption operation on at least one respective bit in the first encrypted data stream and at least one respective bit in the at least weakly random data stream.

20. The system of Claim 19, wherein each of the plurality of bits in the second encrypted data stream is determined at a respective point in the first time interval by performing the encryption operation on at least one bit in the first encrypted data stream generated at an earlier point in the time interval and at least one bit in the at least weakly random data stream.

21. An integrated system, comprising:

an authorization device that generates a first encrypted data stream;

an integrated circuit device that generates a second encrypted data stream and performs first operations during a first time interval; and

authorization detection circuitry that at least periodically compares the first and second encrypted data streams during the first time interval and disables operation of said integrated circuit device if the first and second encrypted data streams indicate that said integrated circuit device is not authorized to perform the first operations.

22. The system of Claim 21, wherein said integrated circuit device generates an at least weakly random data stream during the first time interval; and wherein said authorization device generates the first encrypted data stream in response to the at least weakly random data stream.

23. The system of Claim 21, wherein said authorization detection circuitry is internal to said integrated circuit device; wherein said integrated circuit device utilizes an encryption operation to generate the second encrypted data stream; and wherein each of a plurality of bits in the second encrypted data stream is determined by evaluating at least one bit in the first encrypted data stream.

24. The system of Claim 22, wherein said authorization detection circuitry operates as a dead man switch internal to said integrated circuit device; wherein said integrated circuit device utilizes an encryption operation to generate the second encrypted data stream; and wherein each of a plurality of bits in the second encrypted data stream is determined by performing the encryption operation on at least one respective bit in the first encrypted data stream and at least one respective bit in the at least weakly random data stream.

25. The system of Claim 22, wherein said authorization device and said integrated circuit device are electrically connected together by a bus; and wherein the at least weakly random data stream is time division multiplexed on the bus with the first encrypted data stream.

26. A method of operating a programmable logic device, comprising the steps of:

generating first and second encrypted data streams in first and second devices, respectively, while simultaneously operating the programmable logic device configured to perform a first operation during a first time interval; and

evaluating the first and second encrypted data streams at least periodically during the first time interval and disabling operation of the programmable logic device during a subsequent second time interval if a comparison of the first and second data streams indicate that the programmable logic device is not authorized to perform the first operation.

27. The method of Claim 26, further comprising the step of generating an at least weakly random data stream during the first time interval; and wherein the first and second encrypted data streams are generated from the at least weakly random data stream.

28. The method of Claim 27, wherein the first encrypted data stream is generated internal to the programmable logic device and the second encrypted data stream is generated external to the programmable logic device.

29. The method of Claim 28, wherein the at least weakly random data stream is generated internal to the programmable logic device; wherein the at least weakly random data stream is provided by a single wire bus to a device external to the programmable logic device; and wherein the at least weakly random data stream is time division multiplexed on the bus with the second encrypted data stream.

30. The method of Claim 29, wherein the at least weakly random data stream is generated by mixing clock and noise signals.

31. The method of Claim 29, wherein each of a plurality of bits in the first encrypted data stream is evaluated by performing an encryption operation on a respective bit in the at least weakly random data stream and a respective plurality of bits in second encrypted data stream.

32. An authorization device, comprising:

a first integrated circuit component that in response to a first data stream generated external to said first component generates a second data stream that is at least periodically evaluated by a distinct second integrated circuit component to assess whether performance of operations within the second integrated circuit component are authorized during a time interval when the first data stream is being generated.

33. The device of Claim 32, wherein the first and second data streams are time division multiplexed on an I/O pin associated with said first integrated circuit component.

34. The device of Claim 32, wherein the second data stream is an encrypted data stream; and wherein each of a plurality of bits within the second data stream is generated within said first integrated circuit component using an encryption operation that is a function of at least one bit in the first data stream and at least one bit in the second data stream.

35. The device of Claim 32, wherein the second data stream is an encrypted data stream; and wherein a first encrypted bit within the second data stream is generated within said first integrated circuit component using an encryption operation that is a function of at least one bit in the first data stream and a plurality of previously generated encrypted bits in the second data stream.

36. The device of Claim 35, wherein said first integrated circuit component comprises circuitry that intentionally inserts random errors into the second encrypted data stream.

37. An integrated circuit system, comprising:

a first component that in response to a first data stream generated external to said first component generates a second encrypted data stream; and

a second component that at least periodically evaluates the second encrypted data stream to assess whether performance of at least one operation within the second component is authorized during a time interval when the first data stream is being generated.

38. The system of Claim 37, wherein said second component comprises an integrated circuit selected from the group consisting of ASICs and PLDs.

39. The system of Claim 37, wherein said second component generates the first data stream; and wherein said first and second components comprise first and second stream encryptors therein, respectively.

40. The system of Claim 37, wherein said first and second components are electrically connected together by a single wire bus; and wherein the first data stream and the second encrypted data stream are time division multiplexed on the single wire bus.

41. The system of Claim 39, wherein said first and second components are electrically connected together by a single wire bus; and wherein the first data stream and the second encrypted data stream are time division multiplexed on the single wire bus.

42. The system of Claim 41, wherein said first component comprises circuitry that intentionally inserts random errors into the second encrypted data stream.

43. The system of Claim 39, wherein the second encryptor within said second component generates a third encrypted data stream; and wherein said second component comprises circuitry that operates as a deadman switch to disable performance of the at least one operation within said second component if the second and third encrypted data streams fail to indicate that said second component is authorized by said first component to perform the at least one operation.

44. An integrated circuit system, comprising:

first and second integrated circuit devices that generate first and second data streams, respectively, while said first integrated circuit device performs software and/or hardware controlled operations, said first integrated circuit device having authorization detection circuitry therein that receives and at least periodically evaluates the first and second data streams and disables the software and/or hardware controlled operations when the first and second data streams fail to indicate a sufficient match between said second integrated circuit device and the software and/or hardware controlled operations performed by said first integrated circuit device.

45. The system of Claim 44, wherein said first and second integrated circuit devices generate the first and second data streams in response to an at least weakly random sequence of bits.

46. The system of Claim 45, wherein said first and second integrated circuit devices are electrically coupled together by a single wire bus; and wherein the at least weakly random sequence of bits and the second data stream are time division multiplexed on the single wire bus.

47. The system of Claim 46, wherein said first integrated circuit device comprises a first stream encryptor that generates the first data stream as a first encrypted data stream from the at least weakly random sequence of bits; and wherein said second integrated circuit device comprises a second stream encryptor that generates the second data stream as a second encrypted data stream from the at least weakly random sequence of bits.

48. The system of Claim 47, wherein said first integrated circuit device comprises authorization detection circuitry that generates an error history from the first and second encrypted data streams.

49. The system of Claim 48, wherein said second integrated circuit device comprises circuitry that intentionally inserts random errors into the second encrypted data stream.

50. The system of Claim 45, wherein said first integrated circuit device generates the at least weakly random sequence of bits and comprises a first stream encryptor that generates the first data stream as a first encrypted data stream from the at least weakly random sequence of bits and the second data stream; and wherein said second integrated circuit device comprises a second stream encryptor that generates the second data stream as a second encrypted data stream from the at least weakly random sequence of bits.